

Planned list of Activities And Validation Process For Execution of VAPT

STRYKER, INDIA



Planned list of Activities and Validation Process for Execution of VAPT

Warning: THIS DOCUMENT MAY CONTAIN INFORMATION THAT COULD SEVERELY DAMAGE OR IMPACT THE INTEGRITY AND SECURITY OF THE ORGANIZATION IF DISCLOSED PUBLICLY. THIS DOCUMENT SHOULD BE SAFEGUARDED AT ALL TIMES AND MAINTAINED IN A SECURE AREA WHEN NOT IN USE. G'SECURE LABS ASSUMES NO RESPONSIBILITY OR LIABILITY FOR THE SECURITY OF THIS DOCUMENT AFTER DELIVERY TO THE ORGANIZATION NAMED HEREIN. IT IS THE ORGANIZATION'S RESPONSIBILITY TO SAFEGUARD THIS MATERIAL AFTER DELIVERY.

THIS REPORT CONTAINS PROPRIETARY INFORMATION THAT IS NOT TO BE SHARED, COPIED, DISCLOSED OR OTHERWISE DIVULGED WITHOUT THE EXPRESS WRITTEN CONSENT OF G' SECURE LABS OR THEIR DESIGNATED REPRESENTATIVE. USE OF THIS REPORTING FORMAT BY OTHER THAN G' SECURE LABS OR ITS SUBSIDIARIES IS STRICTLY PROHIBITED AND MAY BE PROSECUTED TO THE FULLEST EXTENT OF THE LAW.

Disclaimer: THE RECOMMENDATIONS CONTAINED IN THIS REPORT ARE BASED ON INDUSTRY STANDARD "BEST PRACTICES". BEST PRACTICES ARE, BY NECESSITY, GENERIC IN NATURE AND MAY NOT TAKE INTO ACCOUNT EXACERBATING OR MITIGATING CIRCUMSTANCES. THESE RECOMMENDATIONS, EVEN IF CORRECTLY APPLIED, MAY CAUSE CONFLICTS IN THE OPERATING SYSTEM OR INSTALLED APPLICATIONS, ANY RECOMMENDED CHANGES TO THE OPERATING SYSTEM OR INSTALLED APPLICATION SHOULD FIRST BE EVALUATED IN A NON-PRODUCTION ENVIRONMENT BEFORE BEING DEPLOYED IN THE PRODUCTION ENVIRONMENT.

G' SECURE LABS



www.gsecurelabs.com

Recipient:

Name/role	Company
Deepak	Stryker

Document Version:

Name of the Author	Version	Title	Date
Arunesh Mishra	1.0	Planned list of Activities And Validation Process For	April 7th, 2022
Arunesh Mishra 1.0		Execution of VAPT	April 7til, 2022
Arunesh Mishra	2.0	Planned list of Activities And Validation Process For	April 11th, 2022
Arunesh Mishra	2.0	Execution of VAPT	



www.gsecurelabs.com

Table of Contents

1.	Summary	••••••	•••••	•••••	•••••	
2.	Planned List of Activities and Validation Process					!
3.	Requirements- Test Cases					45







1. Summary

Stryker has assigned the task of carrying out vulnerability assessment and penetration testing of their SmartMedic Platform by G'Secure Labs team. This is planned list of activities and validation process for execution of VAPT task. The version 1.0 detailed planned list of activities described about each validation process task.

2. Planned List of Activities and Validation Process

Threat Event(s)	Vulnerabilities	Asset	TC No.	Planned list of Activities And Validation Process For Execution of VAPT
Deliver undirected malware (CAPEC-185)	Unprotected external USB Port on the tablet/devices.	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	ST No 01	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Deliver undirected malware (CAPEC-185)	Unprotected external USB Port on the tablet/devices.	Smart medic (Stryker device) System Component	TC No 02	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.







Deliver	External	Smart medic (Stryker device)	TC No	1) Create Android malware
undirected	communications and	System Component	03	2) Transfer the malware to
malware	exposure for	System component	03	•
(CAPEC-185)	communciation			tablet/Smart Medic Device
(channels from and to			3) Malware execution on the device
	application and			4) Exploit the devices with respect to
	devices like tablet and			vulnerability
	smartmedic device.			5) Check for the open ports
				6) Exploit the open ports found while assessment and information
				gathering.
				7) Vulnerability Assessment scanning
				for the identifying unknown
				vulnerabilities
				8) Exploit the found loopholes while
				VA scanning using kali tools.
Deliver	External	Tablet Resources - web cam,	TC No	1) Create Android malware
undirected	communications and	microphone, OTG devices,	04	2) Transfer the malware to
malware (CAPEC-185)	exposure for communciation	Removable USB, Tablet Application, Network interfaces		tablet/Smart Medic Device
(CAPEC-163)	channels from and to	(Bluetooth, Wifi)		3) Malware execution on the device
	application and	(Blactootii, Will)		4) Exploit the devices with respect to
	devices like tablet and			vulnerability
	smartmedic device.			5) Check for the open ports
				6) Exploit the open ports found while
				assessment and information
				gathering.
				7) Vulnerability Assessment scanning
				for the identifying unknown
				vulnerabilities
				8) Exploit the found loopholes while
				VA scanning using kali tools.
Deliver	Legacy system	Smart medic (Stryker device)	TC No	Create Android malware
undirected	identification if any	System Component	05	2) Transfer the malware to
malware	,			tablet/Smart Medic Device
(CAPEC-185)				3) Malware execution on the device
				4) Exploit the devices with respect to
				vulnerability
				5) Check for the open ports
				6) Exploit the open ports found while
				assessment and information
				gathering.
				7) Vulnerability Assessment scanning
				for the identifying unknown
				vulnerabilities
				8) Exploit the found loopholes while
				VA scanning using kali tools.







Deliver undirected malware (CAPEC-185)	Legacy system identification if any	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	TC No 06	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Deliver undirected malware (CAPEC-185)	Ineffective patch management of firware, OS and applications thoughout the information system plan	Device Maintainence tool (Hardware/Software)	TC No 07	NA
Deliver undirected malware (CAPEC-185)	Ineffective patch management of firware, OS and applications thoughout the information system plan	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	TC No 08	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Deliver undirected malware (CAPEC-185)	Ineffective patch management of firware, OS and applications thoughout the information system plan	Smart medic (Stryker device) System Component	TC No 09	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown





Deliver undirected malware	Lack of plan for periodic Software Vulnerability	Device Maintainence tool (Hardware/Software)	TC No 10	vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. NA
(CAPEC-185) Deliver undirected malware (CAPEC-185)	Management Lack of plan for periodic Software Vulnerability Management	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	TC No 11	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Deliver undirected malware (CAPEC-185)	Lack of plan for periodic Software Vulnerability Management	Smart medic (Stryker device) System Component	TC No 12	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Deliver undirected malware (CAPEC-185)	Unprotected network port(s) on network devices and connection points	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	TC No 13	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.







				7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Deliver undirected malware (CAPEC-185)	Unprotected network port(s) on network devices and connection points	Smart medic (Stryker device) System Component	TC No 14	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Deliver undirected malware (CAPEC-185)	Unencrypted data at rest in all possible locations	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	TC No 15	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. 9) Use sniffing tool to sniff the data at motion and MITM
Deliver undirected malware (CAPEC-185)	Unencrypted data in flight in all flowchannels	Smart medic (Stryker device) System Component	TC No 16	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering.







				7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Deliver undirected malware (CAPEC-185)	Unencrypted data in flight in all flowchannels	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	TC No 17	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Deliver undirected malware (CAPEC-185)	Outdated - Software/Hardware	Device Maintainence tool (Hardware/Software)	TC No 18	NA
Deliver undirected malware (CAPEC-185)	Outdated - Software/Hardware	Smart medic (Stryker device) System Component	TC No 19	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Deliver undirected malware (CAPEC-185)	Outdated - Software/Hardware	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	TC No 20	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while







Deliver directed malware (CAPEC-185)	InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers	Device Maintainence tool (Hardware/Software)	TC No 21	assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. NA
Deliver directed malware (CAPEC-185)	InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers	Smart medic (Stryker device) System Component	TC No 22	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Deliver directed malware (CAPEC-185)	InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	TC No 23	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Deliver directed malware (CAPEC-185)	Unprotected external USB Port on the tablet/devices.	Wireless Network device	TC No 24	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device





Deliver directed malware (CAPEC-185)	Unprotected external USB Port on the tablet/devices.	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	TC No 25	4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Use sniffing tool to sniff the data at motion and MITM 7) Exploit the open ports found while assessment and information gathering. 8) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 9) Exploit the found loopholes while VA scanning using kali tools. 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Deliver directed malware (CAPEC-185)	Unprotected external USB Port on the tablet/devices.	Smart medic app (Stryker Azure Cloud Web Application)	TC No 26	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Deliver directed malware (CAPEC-185)	External communications and exposure for communciation channels from and to application and devices like tablet and smartmedic device.	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	TC No 27	 Create Android malware Transfer the malware to tablet/Smart Medic Device Malware execution on the device Exploit the devices with respect to vulnerability Check for the open ports Exploit the open ports found while assessment and information





				gathering.
				7) Vulnerability Assessment scanning
				for the identifying unknown
				vulnerabilities
				8) Exploit the found loopholes while
				VA scanning using kali tools.
Deliver directed	Ineffective patch	Device Maintainence tool	TC No	NA
malware	management of	(Hardware/Software)	28	
(CAPEC-185)	firware, OS and			
	applications thoughout			
	the information			
Deliver directed	system plan	Smart madia (Strukar davisa)	TC No	1) Create Andreid maluere
malware	Ineffective patch management of	Smart medic (Stryker device) System Component	29	1) Create Android malware
(CAPEC-185)	firware, OS and	System component	29	2) Transfer the malware to
(3. 1. 2. 2. 2. 2. 7	applications thoughout			tablet/Smart Medic Device
	the information			3) Malware execution on the device
	system plan			4) Exploit the devices with respect to
				vulnerability 5) Check for the open ports
				6) Exploit the open ports found while
				assessment and information
				gathering.
				7) Vulnerability Assessment scanning
				for the identifying unknown vulnerabilities
				8) Exploit the found loopholes while
Deliver directed	Ineffective patch	Tablet Resources - web cam,	TC No	VA scanning using kali tools. 1) Create Android malware
malware	management of	microphone, OTG devices,	30	2) Transfer the malware to
(CAPEC-185)	firware, OS and	Removable USB, Tablet	30	tablet/Smart Medic Device
	applications thoughout	Application, Network interfaces		3) Malware execution on the device
	the information	(Bluetooth, Wifi)		4) Exploit the devices with respect to
	system plan			vulnerability
				5) Check for the open ports
				6) Exploit the open ports found while
				assessment and information
				gathering.
				7) Vulnerability Assessment scanning
				for the identifying unknown
				vulnerabilities
				8) Exploit the found loopholes while
				VA scanning using kali tools.
Deliver directed	Unprotected network	Smart medic (Stryker device)	TC No	Create Android malware
malware	port(s) on network	System Component	31	2) Transfer the malware to
(CAPEC-185)	devices and			tablet/Smart Medic Device
	connection points			3) Malware execution on the device
				4) Exploit the devices with respect to
				1, Exploit the devices with respect to







			Ī	
				vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Deliver directed malware (CAPEC-185)	Unprotected network port(s) on network devices and connection points	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	TC No 32	 Create Android malware Transfer the malware to tablet/Smart Medic Device Malware execution on the device Exploit the devices with respect to vulnerability Check for the open ports Exploit the open ports found while assessment and information gathering. Vulnerability Assessment scanning for the identifying unknown vulnerabilities Exploit the found loopholes while Scanning using kali tools.
Deliver directed malware (CAPEC-185)	Unprotected network port(s) on network devices and connection points	Wireless Network device	TC No 33	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Use sniffing tool to sniff the data at motion and MITM 7) Exploit the open ports found while assessment and information gathering. 8) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 9) Exploit the found loopholes while VA scanning using kali tools.
Deliver directed malware (CAPEC-185)	InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers	Smart medic app (Stryker Azure Cloud Web Application)	TC No 34	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools





				3) Exploit the found loopholes while
				VA Scanning using the Burpsuite, kali
				tools.
				4) Exploit the open ports using kali
				tools.
Deliver directed	InSecure Configuration	Tablet Resources - web cam,	TC No	1) Create Android malware
malware	for Software/OS on	microphone, OTG devices,	35	2) Transfer the malware to
(CAPEC-185)	Mobile Devices, Laptops, Workstations,	Removable USB, Tablet Application, Network interfaces		tablet/Smart Medic Device
	and Servers	(Bluetooth, Wifi)		3) Malware execution on the device
				4) Exploit the devices with respect to
				vulnerability 5) Check for the open ports
				6) Exploit the open ports found while
				assessment and information
				gathering.
				7) Vulnerability Assessment scanning
				for the identifying unknown
				vulnerabilities
				8) Exploit the found loopholes while
				VA scanning using kali tools.
Deliver directed	Unencrypted data at	Tablet Resources - web cam,	TC No	1) Create Android malware
malware (CAPEC-185)	rest in all possible locations	microphone, OTG devices, Removable USB, Tablet	36	2) Transfer the malware to
(CAI LC 103)	locations	Application, Network interfaces		tablet/Smart Medic Device
		(Bluetooth, Wifi)		3) Malware execution on the device4) Exploit the devices with respect to
				vulnerability
				5) Check for the open ports
				6) Exploit the open ports found while
				assessment and information
				gathering.
				7) Vulnerability Assessment scanning
				for the identifying unknown
				vulnerabilities
				8) Exploit the found loopholes while
				VA scanning using kali tools.
				9) Use sniffing tool to sniff the data
Deliver directed	Unencrypted data at	Tablet OS/network details &	TC No	at motion and MITM 1) Create Android malware
malware	rest in all possible	Tablet Application	37	2) Transfer the malware to
(CAPEC-185)	locations			tablet/Smart Medic Device
				3) Malware execution on the device
				4) Exploit the devices with respect to
				vulnerability
				5) Check for the open ports
				6) Exploit the open ports found while
				assessment and information
				gathering.





				7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. 9) Use sniffing tool to sniff the data at motion and MITM
Deliver directed malware (CAPEC-185)	Unencrypted data at rest in all possible locations	Smart medic app (Stryker Azure Cloud Web Application)	TC No 38	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Use sniffing tool to sniff the data at motion and MITM
Gaining Access ([S]TRID[E])	Unprotected network port(s) on network devices and connection points	Tablet OS/network details & Tablet Application	TC No 39	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Gaining Access ([S]TRID[E])	Unprotected network port(s) on network devices and connection points	Smart medic app (Stryker Azure Cloud Web Application)	TC No 40	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Gaining Access ([S]TRID[E])	Unprotected network port(s) on network	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet	TC No 41	Create Android malware Transfer the malware to tablet/Smart Medic Device





	devices and connection points	Application, Network interfaces (Bluetooth, Wifi)		3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Gaining Access ([S]TRID[E])	Devices with default passwords needs to be checked for bruteforce attacks	Authenication/Authorisation data	TC No 42	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port
Gaining Access ([S]TRID[E])	Devices with default passwords needs to be checked for bruteforce attacks	Smart medic app (Stryker Azure Cloud Web Application)	TC No 43	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Gaining Access ([S]TRID[E])	Devices with default passwords needs to be checked for bruteforce attacks	Interface/API Communication	TC No 44	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools.







				4) Exploit the open ports using kali tools.
Gaining Access ([S]TRID[E])	The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	Authenication/Authorisation data	TC No 45	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port
Gaining Access ([S]TRID[E])	The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	Smart medic app (Stryker Azure Cloud Web Application)	TC No 46	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Gaining Access ([S]TRID[E])	The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	Smart medic app (Azure Portal Administrator)	TC No 47	 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Gaining Access ([S]TRID[E])	Checking authentication modes for possible hacks and bypasses	Authenication/Authorisation data	TC No 48	 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali







				tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port
Gaining Access ([S]TRID[E])	Checking authentication modes for possible hacks and bypasses	Smart medic app (Stryker Azure Cloud Web Application)	TC No 49	 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Gaining Access ([S]TRID[E])	Checking authentication modes for possible hacks and bypasses	Smart medic app (Azure Portal Administrator)	TC No 50	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Gaining Access ([S]TRID[E])	Controlled Use of Administrative Privileges over the network	Authenication/Authorisation data	TC No 51	 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port





Gaining Access ([S]TRID[E])	Controlled Use of Administrative Privileges over the network	Smart medic app (Azure Portal Administrator)	TC No 52	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Gaining Access ([S]TRID[E])	Unprotected external USB Port on the tablet/devices.	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	TC No 53	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Maintaining Access (TTP)	Devices with default passwords needs to be checked for bruteforce attacks	Smart medic app (Stryker Azure Cloud Web Application)	TC No 54	 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Maintaining Access (TTP)	Devices with default passwords needs to be checked for bruteforce attacks	Smart medic app (Azure Portal Administrator)	TC No 55	 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.







Maintaining	Devices with default	Authenication/Authorisation	TC No	1) Vulnerability Assessment scanning
Access (TTP)	passwords needs to be checked for bruteforce attacks	data	56	for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port
Maintaining Access (TTP)	The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	Smart medic app (Stryker Azure Cloud Web Application)	TC No 57	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Maintaining Access (TTP)	The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	Smart medic app (Azure Portal Administrator)	TC No 58	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Maintaining Access (TTP)	The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	Authenication/Authorisation data	TC No 59	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.





			I	5) 5
				5) Brute Force attempt for the
				authentication/authorization on the
				open port
				6) Exploit related to Brute Force
				attempt for the
				authentication/authorization on the
NA-intain'	Charlina	Constitution of Constitution o	TCN	open port
Maintaining Access	Checking authentication modes	Smart medic app (Stryker Azure Cloud Web Application)	TC No	1) Vulnerability Assessment scanning
(TTP)	for possible hacks and	Cloud Web Application)	60	for the identifying unknown
\ <i>j</i>	bypasses			vulnerabilities of web application.
	,,			2) Check for the open ports using
				nmap, other kali tools
				3) Exploit the found loopholes while
				VA Scanning using the Burpsuite, kali
				tools.
				4) Exploit the open ports using kali
Maintainina	Charling	Cusant madia and (Anuma Dantal	TCNa	tools.
Maintaining Access	Checking authentication modes	Smart medic app (Azure Portal Administrator)	TC No 61	Vulnerability Assessment scanning for the identifying unknown
(TTP)	for possible hacks and	Administratory	01	
(,	bypasses			vulnerabilities of web application.
				2) Check for the open ports using
				nmap, other kali tools
				3) Exploit the found loopholes while
				VA Scanning using the Burpsuite, kali tools.
				4) Exploit the open ports using kali
				tools.
Maintaining	Controlled Use of	Smart medic app (Azure Portal	TC No	1) Vulnerability Assessment scanning
Access	Administrative	Administrator)	62	for the identifying unknown
(TTP)	Privileges over the		"-	vulnerabilities of web application.
	network			2) Check for the open ports using
				nmap, other kali tools
				3) Exploit the found loopholes while
				VA Scanning using the Burpsuite, kali
				tools.
				4) Exploit the open ports using kali
				tools.
Maintaining	Controlled Use of	Authenication/Authorisation	TC No	1) Vulnerability Assessment scanning
Access	Administrative	data	63	for the identifying unknown
(TTP)	Privileges over the			vulnerabilities of web application.
	network			2) Check for the open ports using
				nmap, other kali tools
				3) Exploit the found loopholes while
				VA Scanning using the Burpsuite, kali
				tools.
				4) Exploit the open ports using kali
				tools.
				100101





			ı	
				5) Brute Force attempt for the
				authentication/authorization on the
				open port
				6) Exploit related to Brute Force
				attempt for the
				authentication/authorization on the
				open port
Clearing Track	InSecure Configuration	Tablet Resources - web cam,	TC No	1) Create Android malware
(TTP)	for Software/OS on	microphone, OTG devices,	64	2) Transfer the malware to
	Mobile Devices,	Removable USB, Tablet		tablet/Smart Medic Device
	Laptops, Workstations, and Servers	Application, Network interfaces (Bluetooth, Wifi)		3) Malware execution on the device
	and Servers	(Bidetootii, Wiii)		4) Exploit the devices with respect to
				vulnerability
				5) Check for the open ports
				6) Exploit the open ports found while
				assessment and information
				gathering.
				7) Vulnerability Assessment scanning
				for the identifying unknown
				vulnerabilities
				8) Exploit the found loopholes while
				VA scanning using kali tools.
Clearing Track	InSecure Configuration	Smart medic app (Stryker Azure	TC No	Vulnerability Assessment scanning
(TTP)	for Software/OS on	Cloud Web Application)	65	for the identifying unknown
(***)	Mobile Devices,	риссии,	03	vulnerabilities of web application.
	Laptops, Workstations,			2) Check for the open ports using
	and Servers			nmap, other kali tools
				3) Exploit the found loopholes while
				• •
				VA Scanning using the Burpsuite, kali
				tools.
				4) Exploit the open ports using kali
				tools.
Clearing Track	Outdated -	Tablet Resources - web cam,	TC No	1) Create Android malware
(TTP)	Software/Hardware	microphone, OTG devices,	66	2) Transfer the malware to
		Removable USB, Tablet Application, Network interfaces		tablet/Smart Medic Device
		(Bluetooth, Wifi)		3) Malware execution on the device
		(Bidetootii, Wiii)		4) Exploit the devices with respect to
				vulnerability
				5) Check for the open ports
				6) Exploit the open ports found while
				assessment and information
				gathering.
				7) Vulnerability Assessment scanning
				for the identifying unknown
				vulnerabilities
				8) Exploit the found loopholes while
			1	VA scanning using kali tools.





61 1		T.11.15	TC 1:	4) 6
Clearing Track (TTP)	Lack of configuration controls for IT assets in the informaion system plan	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	TC No 67	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Clearing Track (TTP)	Lack of configuration controls for IT assets in the informaion system plan	Device Maintainence tool (Hardware/Software)	TC No 68	NA
Clearing Track (TTP)	Ineffective patch management of firware, OS and applications thoughout the information system plan	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	TC No 69	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Clearing Track (TTP)	Ineffective patch management of firware, OS and applications thoughout the information system plan	Device Maintainence tool (Hardware/Software)	TC No 70	NA
Clearing Track (TTP)	Ineffective patch management of firware, OS and applications thoughout the information system plan	Tablet OS/network details & Tablet Application	TC No 71	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability





				 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Clearing Track (TTP)	The static connection digaram between devices and applications with provision for periodic updation as per changes	Device Maintainence tool (Hardware/Software)	TC No 72	NA
Clearing Track (TTP)	The static connection digaram between devices and applications with provision for periodic updation as per changes	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	TC No 73	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Elevation of privilege (STRID[E])	Controlled Use of Administrative Privileges over the network	Authenication/Authorisation data	TC No 74	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port





Elevation of privilege (STRID[E])	Controlled Use of Administrative Privileges over the network	Smart medic app (Azure Portal Administrator)	TC No 75	 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while
Denial of service	Unprotected network	Wireless Network device	TC No	VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 1) Create Android malware
(STRI(D)E)	port(s) on network devices and connection points		76	2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Use sniffing tool to sniff the data at motion and MITM 7) Exploit the open ports found while assessment and information gathering. 8) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 9) Exploit the found loopholes while VA scanning using kali tools.
Denial of service (STRI(D)E)	Unprotected network port(s) on network devices and connection points	Tablet OS/network details & Tablet Application	TC No 77	 1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Information disclosure (STR(I)DE)	Unencrypted data at rest in all possible locations	Data at Rest	TC No 78	 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools





Information	Unencrypted data in	Data in Motion	TC No	3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM 8) Use sniffing tool to sniff the data at motion and MITM 1) Vulnerability Assessment scanning
disclosure (STR(I)DE)	flight in all flowchannels	Data III IVIOLIOII	79	for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM
Information disclosure (STR(I)DE)	Weak Encryption Implementaion in data at rest and in motion tactical and design wise	Data at Rest	TC No 80	 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the





				open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM
Information disclosure (STR(I)DE)	Weak Encryption Implementaion in data at rest and in motion tactical and design wise	Data in Motion	TC No 81	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM
Information disclosure (STR(I)DE)	Weak Algorthim implementation with respect cipher key size	Data at Rest	TC No 82	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM







Information disclosure (STR(I)DE)	Weak Algorthim implementation with respect cipher key size	Data in Motion	TC No 83	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the
				authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM
Information disclosure (STR(I)DE)	InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	TC No 84	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Information disclosure (STR(I)DE)	Unencrypted Network segment throught the information flow	Data in Motion	TC No 85	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port







				6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM
Information disclosure (STR(I)DE)	Insecure communications in networks (hospital)	Data in Motion	TC No 86	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM
Data Access (STR[I]DE)	Unprotected network port(s) on network devices and connection points	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	TC No 87	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Data Access (STR[I]DE)	Unprotected network port(s) on network devices and connection points	Wireless Network device	TC No 88	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports







				6) Use sniffing tool to sniff the data at motion and MITM 7) Exploit the open ports found while assessment and information gathering. 8) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 9) Exploit the found loopholes while VA scanning using kali tools.
Data Access (STR[I]DE)	Unprotected network port(s) on network devices and connection points	Tablet OS/network details & Tablet Application	TC No 89	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Data Access (STR[I]DE)	Devices with default passwords needs to be checked for bruteforce attacks	Data at Rest	TC No 90	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM
Data Access (STR[I]DE)	Devices with default passwords needs to be	Authenication/Authorisation data	TC No 91	Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application.







	checked for bruteforce attacks			2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port
Data Access (STR[I]DE)	Devices with default passwords needs to be checked for bruteforce attacks	Data in Motion	TC No 92	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM
Data Access (STR[I]DE)	The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	Data at Rest	TC No 93	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force







				attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM
Data Access (STR[I]DE)	The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	Smart medic app (Azure Portal Administrator)	TC No 94	 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Data Access (STR[I]DE)	Controlled Use of Administrative Privileges over the network	Smart medic app (Azure Portal Administrator)	TC No 95	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Data Access (STR[I]DE)	Unprotected external USB Port on the tablet/devices.	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	TC No 96	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Open network port exploit (TTP)	Unprotected network port(s) on network devices and connection points	Tablet OS/network details & Tablet Application	TC No 97	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports







				6) = 1 1111
				6) Exploit the open ports found while
				assessment and information
				gathering.
				7) Vulnerability Assessment scanning
				for the identifying unknown
				vulnerabilities
				8) Exploit the found loopholes while
				VA scanning using kali tools.
Open network	Unprotected network	Wireless Network device	TC No	1) Create Android malware
port exploit	port(s) on network		98	2) Transfer the malware to
(TTP)	devices and			tablet/Smart Medic Device
	connection points			3) Malware execution on the device
				4) Exploit the devices with respect to
				vulnerability
				5) Check for the open ports
				6) Use sniffing tool to sniff the data
				at motion and MITM
				7) Exploit the open ports found while
				assessment and information
				gathering.
				8) Vulnerability Assessment scanning
				for the identifying unknown
				vulnerabilities
				9) Exploit the found loopholes while
				VA scanning using kali tools.
Onan naturali	Unananintad Naturali	Tablet OS/network details &	TC No	Create Android malware
Open network port exploit	Unencrypted Network segment throught the	Tablet Application		•
(TTP)	information flow	rubict Application	99	2) Transfer the malware to
(,				tablet/Smart Medic Device
				3) Malware execution on the device
				4) Exploit the devices with respect to
				vulnerability
				5) Check for the open ports
				6) Exploit the open ports found while
				assessment and information
				gathering.
				7) Vulnerability Assessment scanning
				for the identifying unknown
				vulnerabilities
				8) Exploit the found loopholes while
				VA scanning using kali tools.
Open network	Unencrypted Network	Wireless Network device	TC No	1) Create Android malware
port exploit	segment throught the		100	2) Transfer the malware to
(TTP)	information flow			tablet/Smart Medic Device
				3) Malware execution on the device
				4) Exploit the devices with respect to
				vulnerability
				5) Check for the open ports
			l .	1 1 2 22





	6) Use sniffing tool to sniff the data
	at motion and MITM
	7) Exploit the open ports found while
	assessment and information
	gathering.
	8) Vulnerability Assessment scanning
	for the identifying unknown
	vulnerabilities
	9) Exploit the found loopholes while
	VA scanning using kali tools.
Open network Controlled Use of Smart medic app (Azure Portal TC N	,
port exploit Administrative Administrator) Administrator) Administrator)	for the identifying unknown
(TTP) Privileges over the network	vulnerabilities of web application.
network	2) Check for the open ports using
	nmap, other kali tools
	3) Exploit the found loopholes while
	VA Scanning using the Burpsuite, kali
	tools.
	4) Exploit the open ports using kali
	tools.
Open network Unencrypted data in Data in Motion TC N	Io 1) Vulnerability Assessment scanning
port exploit flight in all	for the identifying unknown
(TTP) flowchannels	vulnerabilities of web application.
	2) Check for the open ports using
	nmap, other kali tools
	3) Exploit the found loopholes while
	VA Scanning using the Burpsuite, kali
	tools.
	4) Exploit the open ports using kali
	tools.
	5) Brute Force attempt for the
	authentication/authorization on the
	open port
	6) Exploit related to Brute Force
	attempt for the
	authentication/authorization on the
	open port
	7) Use sniffing tool to sniff the data
	at motion and MITM
Open network Insecure Tablet OS/network details & TC N	lo 1) Create Android malware
port exploit communications in Tablet Application 103	2) Transfer the malware to
(TTP) networks (hospital)	tablet/Smart Medic Device
	3) Malware execution on the device
	4) Exploit the devices with respect to
	vulnerability
	5) Check for the open ports





Brute-force Attack (CAPEC-112)	Devices with default passwords needs to be checked for bruteforce attacks	Smart medic app (Stryker Azure Cloud Web Application)	TC No 104	assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while
				VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Brute-force Attack (CAPEC-112)	Devices with default passwords needs to be checked for bruteforce attacks	Smart medic app (Azure Portal Administrator)	TC No 105	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Brute-force Attack (CAPEC-112)	Devices with default passwords needs to be checked for bruteforce attacks	Azure Cloud DataBase	TC No 106	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port
Brute-force Attack (CAPEC-112)	The password complexity or location vulnerability. Like	Smart medic app (Stryker Azure Cloud Web Application)	TC No 107	Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application.





	weak passwords and hardcoded passwords.			 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Brute-force Attack (CAPEC-112)	The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	Smart medic app (Azure Portal Administrator)	TC No 108	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Brute-force Attack (CAPEC-112)	The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	Azure Cloud DataBase	TC No 109	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port
Brute-force Attack (CAPEC-112)	Checking authentication modes for possible hacks and bypasses	Smart medic app (Stryker Azure Cloud Web Application)	TC No 110	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Brute-force Attack (CAPEC-112)	Checking authentication modes	Smart medic app (Azure Portal Administrator)	TC No 111	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application.





	for possible hacks and bypasses			 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Brute-force Attack (CAPEC-112)	Weak Encryption Implementaion in data at rest and in motion tactical and design wise	Data at Rest	TC No 112	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM
Brute-force Attack (CAPEC-112)	Weak Encryption Implementaion in data at rest and in motion tactical and design wise	Data in Motion	TC No 113	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM







Cosial	InCoours Configuration	Smort modic and /Starley A	TC No	1) Vulnarability Assessment
Social Engineering (TTP)	InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers	Smart medic app (Stryker Azure Cloud Web Application)	TC No 114	 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Social Engineering (TTP)	Legacy system identification if any	Smart medic app (Stryker Azure Cloud Web Application)	TC No 115	 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Social Engineering (TTP)	The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	Smart medic app (Stryker Azure Cloud Web Application)	TC No 116	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Social Engineering (TTP)	Checking authentication modes for possible hacks and bypasses	Interface/API Communication	TC No 117	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Social Engineering (TTP)	Checking authentication modes for possible hacks and bypasses	Smart medic app (Stryker Azure Cloud Web Application)	TC No 118	 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali





				41-
				tools. 4) Exploit the open ports using kali tools.
Social Engineering (TTP)	Checking authentication modes for possible hacks and bypasses	Azure Cloud DataBase	TC No 119	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port
Social Engineering (TTP)	Checking authentication modes for possible hacks and bypasses	Smart medic app (Azure Portal Administrator)	TC No 120	 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Lack of evidence to conclude any malicious attempt/attack (ST[R]IDE)	Insufficient Logging information	Smart medic app (Azure Portal Administrator)	TC No 121	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Lack of evidence to conclude any malicious attempt/attack (ST[R]IDE)	Insufficient Access permissions for accessing and modifying Log files	Smart medic app (Azure Portal Administrator)	TC No 122	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali





				tools. 4) Exploit the open ports using kali tools.
Unauthorized Alterations (S[T]RIDE)	InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers	Azure Cloud DataBase	TC No 123	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port
Unauthorized Alterations (S[T]RIDE)	Insufficient Access permissions for accessing and modifying Log files	Azure Cloud DataBase	TC No 124	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port
Gaining Access ([S]TRID[E])	Error Info containing sensitive data for Failed Authentication attempts	Smart medic app (Azure Portal Administrator)	TC No 125	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.







Gaining Access ([S]TRID[E])	Error Info containing sensitive data for Failed Authentication attempts	Azure Cloud DataBase	TC No 126	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port
Gaining Access ([S]TRID[E])	Absence of additional security factor along with user identification	Smart medic app (Azure Portal Administrator)	TC No 127	 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Gaining Access ([S]TRID[E])	Absence of additional security factor along with user identification	Azure Cloud DataBase	TC No 128	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port
Gaining Access ([S]TRID[E])	Having no limit on the login attempts	Smart medic app (Azure Portal Administrator)	TC No 129	Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application.







				 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Gaining Access ([S]TRID[E])	Having no limit on the login attempts	Azure Cloud DataBase	TC No 130	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port
Brute-force Attack (CAPEC-112)	Error Info containing sensitive data for Failed Authentication attempts	Smart medic app (Azure Portal Administrator)	TC No 131	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Brute-force Attack (CAPEC-112)	Error Info containing sensitive data for Failed Authentication attempts	Azure Cloud DataBase	TC No 132	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port







			I	6) 5 1 11 1 1 1 5 5
				6) Exploit related to Brute Force attempt for the
				authentication/authorization on the
				open port
Brute-force Attack (CAPEC-112)	Absence of additional security factor along with user identification	Smart medic app (Azure Portal Administrator)	TC No 133	Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application.
				2) Check for the open ports using nmap, other kali tools
				3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali
				tools.
				4) Exploit the open ports using kali tools.
Brute-force Attack	Absence of additional security factor along	Azure Cloud DataBase	TC No	1) Vulnerability Assessment scanning
(CAPEC-112)	with user identification		134	for the identifying unknown vulnerabilities of web application.
				2) Check for the open ports using
				nmap, other kali tools
				3) Exploit the found loopholes while
				VA Scanning using the Burpsuite, kali tools.
				4) Exploit the open ports using kali tools.
				5) Brute Force attempt for the
				authentication/authorization on the open port
				6) Exploit related to Brute Force
				attempt for the
				authentication/authorization on the
				open port
Brute-force Attack (CAPEC-112)	Having no limit on the login attempts	Smart medic app (Azure Portal Administrator)	TC No 135	1) Vulnerability Assessment scanning for the identifying unknown
(CAI LC-112)				vulnerabilities of web application. 2) Check for the open ports using
				nmap, other kali tools
				3) Exploit the found loopholes while
				VA Scanning using the Burpsuite, kali tools.
				4) Exploit the open ports using kali tools.
Brute-force	Having no limit on the	Azure Cloud DataBase	TC No	1) Vulnerability Assessment scanning
Attack (CAPEC-112)	login attempts		136	for the identifying unknown
(3.1.30 222)				vulnerabilities of web application. 2) Check for the open ports using
				nmap, other kali tools
				3) Exploit the found loopholes while





	VA Scanning using the Burpsuite, kali
	tools.
	4) Exploit the open ports using kali
	tools.
	5) Brute Force attempt for the
	authentication/authorization on the
	open port
	6) Exploit related to Brute Force
	attempt for the
	authentication/authorization on the
	open port

3. Requirements- Test Cases

Test Case No.	Test Case Name	Asset
REQ-STC-001	The Application shall support the use of anti-malware mechanism	Tablet
REQ-STC-002	The Application shall provide secure tunnel Communications channel	Tablet SM Device NSA
REQ-STC-003	Only Stryker made/authenticated devices should be able to communicate with SM device and tablet.	Tablet SM Device
REQ-STC-004	The application shall be allowed to upgrade the tablet application.	Admin
REQ-STC-005	Application shall have the User Management Screen to configure and manage the users as per the roles.	Admin
REQ-STC-006	The Application shall be validated by using invisible captcha during login.	NSA
REQ-STC-007	Invalid login creds, only 3 attempts left.	Admin NSA
REQ-STC-008	System shall store patient id in anonymized fashion.	Admin
REQ-STC-009	Error msg: Something went wrong with API operation try again / contact API admin.	Admin NSA
REQ-STC-010	For sensitive data at rest, identification & proper encryption mechanism needs to be designed & implemented	Tablet Cloud db
REQ-STC-011	Secure sensitive data in the channel flow using strong encryption	Tablet Admin
REQ-STC-012	Weak algorithms such as DES, RC4, etc should be avoided and usage of strong algorithms such as AES, RSA, etc are recommended	Tablet Cloud db







REQ-STC-013	Typical key lengths are 128 and 256 bits for private keys and 2048 for public keys are recommended.	Tablet Cloud db
REQ-STC-014	If database access using keys/certificates, their generation & storage should be done securely.	Tablet Cloud db
REQ-STC-015	Weight and patient data in the database shall be available upto 6 months.	NSA
REQ-STC-016	User shall find the overall system flow in the User Manual document.	NSA
REQ-STC-017	The application will be used by the Stryker Installation and service teams.	Admin

*** End of the document

www.gsecurelabs.com







Maria Montessorilaan 3, 2719 DB Zoetermeer, The Netherlands

INDIA

B/81, Corporate House, Judges Bungalow Road, Bodakdev, Ahmedabad - 380054. India

www.gsecurelabs.com

Confidentiality Clause:

This document and any files with it are for the sole use of the intended recipient(s) and may contain confidential and privileged information. If you are not the intended recipient, please destroy all copies of the document. Any unauthorized review, use, disclosure, dissemination, forwarding, printing or copying of this document or any action taken in reliance on this document is strictly prohibited and may be unlawful. Copyright © Gateway Group

